AF JFW

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICANT	:	Jin Lu et al.		
SERIAL NO.	:	09/461,984	EXAMINER	: Brandon S. Hoffman
FILED	:	December 15, 1999	ART UNIT	: 2136
FOR	:	SYSTEM AND METHOD FOR COPY PROTECTING TRANSMITTED INFORMATION		

APPEAL BRIEF TRANSMITTAL LETTER

Mail Stop Appeal Brief-Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA. 22313-1450

Dear Sir:

Appellants respectfully submit three copies of an Appeal Brief For Appellants that includes an Appendix with the pending claims. The Appeal Brief is now due on January 17, 2006 as Monday, January 16, 2006 was a holiday.

Appellants enclose a check in the amount of $500.00 covering the requisite Government Fee.

Should the Examiner deem that there are any issues which may be best resolved by telephone communication, kindly telephone Applicants undersigned representative at the number listed below.

Respectfully submitted,
Dan Piotrowski
Registration No. 42,079

By: Steve Cha
Attorney for Applicant
Registration No. 44,069

Date: January 17, 2006

Mail all correspondence to:
Dan Piotrowski, Registration No. 42,079
US PHILIPS CORPORATION
P.O. Box 3001
Briarcliff Manor, NY 10510-8001
Phone: (914) 333-9608
Fax: (914) 332-0615

Certificate of Mailing Under 37 CFR 1.8

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to MAIL STOP APPEAL BRIEF-PATENTS, COMMISSIONER FOR PATENTS, P.O. BOX 1450, ALEXANDRIA, VA. 22313 on January 17, 2006.

David Rosenblum, Reg No. 37,709
(Name of Registered Rep.)

David J Rosenblum 1/17/06
(Signature and Date)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Before the Board of Patent Appeals and Interferences

In re the Application

Inventor : Jin Lu et al.

Application No. : 09/461,984

Filed : December 15, 1999

For : SYSTEM AND METHOD FOR COPY PROTECTING TRANSMITTED INFORMATION

APPEAL BRIEF

On Appeal from Group Art Unit 2136

Dan Piotrowski
Registration No. 42,079

Date: January 17, 2006

By: Steve Cha
Attorney for Applicant
Registration No. 44,069

Certificate of Mailing Under 37 CFR 1.8

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to MAIL STOP APPEAL BRIEF-PATENTS, COMMISSIONER FOR PATENTS, P.O. BOX 1450, ALEXANDRIA, VA. 22313 on January 17, 2006.

David J. Rosenblum, Reg. No. 37,709
(Name of Registered Rep.)

1/17/06
(Signature and Date)

TABLE OF CONTENTS

I. REAL PARTY IN INTEREST

The real party in interest is the assignee of the present application, U.S. Philips Corporation, and not the party named in the above caption.

II. RELATED APPEALS AND INTERFERENCES

With regard to identifying by number and filing date all other appeals or interferences known to Appellant which will directly effect or be directly affected by or have a bearing on the Board's decision in this appeal, Appellant is not aware of any such appeals or interferences.

III. STATUS OF CLAIMS

Claims 1-29 have been presented for examination. All of these claims are pending, stand finally rejected, and form the subject matter of the present appeal. Claims 2-17 are original. Claims 1 and 18-29 are previously presented.

IV. STATUS OF AMENDMENTS

The Amendment after the Final Office Action filed November 16, 2005 has not been entered.

V. SUMMARY OF CLAIMED SUBJECT MATTER

A system for copy protecting information includes a point of deployment module 12 and a set-top box 10 (FIG. 1, page 1, lines 19-21). The set-top box 10 transmits a request message for information (FIG. 2a, ref. no. 206; page 9, lines 1-11). This transmission might occur when the user actuates the remote control to change channels. In response to the request message, the point of deployment module 12 generates a reply message (FIG. 2a, ref. no. 210) which includes at least one control information pair, relating to the information (page 9, lines 19-24). The information might be multimedia content for the particular channel selected by the user by means of the remote control. Since the multimedia content is conveyed by elementary streams and since, according to a particular protocol, each copy protected elementary stream is associated with respective copy control information (page 2, lines 23-24), each control information pair has copy control information and a stream identifier (page 9, lines 24-26). A first key is generated in the point of deployment module and a second key is generated in the set-top box, each respectively using the at least one control information pair (FIG. 2a, ref. no. 212; page 9, line 27 - page 10, line 1). The point of deployment module encrypts the information with the first shared key and transmits the encrypted information to the set-top box (page 10, lines 1-4). The set-top box decrypts the encrypted information with the second shared key when the first and second shared keys match (page 12, lines 16-28).

To use the at least one control information pair in the generating of the second key, the set-top box receives a transmission of the at least one control information pair. The respective copy control information of the at least one control information pair is not encrypted for the transmission (page 3, lines 12-14; page 12, line 30 - page 13, line 9).

VI. GROUNDS FOR REJECTION TO BE REVIEWED ON APPEAL

Whether claims 1-29 stand invalidly rejected under 35 U.S.C. 103(a) as unpatentable over U.S. Patent No. 5,799,081 to Kim et al. ("Kim") in view of U.S. Patent No. 6,550,008 to Zhang et al. ("Zhang") and ITU-T Recommendation H.222.0 (hereinafter "ITU-T").

VII. ARGUMENT

Rejection of claims 1-18 and 22-29

Claim 1 recites:

> the set-top box transmits a request message for information, the point of deployment module generates a reply message which includes at least one control information pair, relating to the information, each control information pair having copy control information and a stream identifier, respectively generating a first key in the point of deployment module and a second key in the set-top box, using the at least one control information pair, and the point of deployment module encrypting the information with the first shared key and transmitting the encrypted information to the set-top box, and the set-top box decrypting the encrypted information with the second shared key when the first and second shared keys match

Kim fails to disclose or suggest at least the "stream identifier" of claim 1 and the feature ". . . when the first and second shared keys match."

At the top of page 3 of the Office Action are four items denoted by respective bullets. The second item suggests that the Office Action regards the reply message of the present claim 1 as corresponding to a pair of data. The pair of data consists of the control word CW and "signal for controlling copy protection" (col. 18, line 50) CP transmitted from smart card 261 to controller 262 (Kim, FIG. 21; Zhang, col. 3, lines 14-19: "The POD module 26 may be a . . . smart card").

However, claim 1 provides that the reply message "includes at least one control information pair, relating to the information, each control information pair having copy control information and a stream identifier."

The third bullet on page 3 of the Office Action seems to suggest that the "stream identifier" is disclosed in lines 46-48 at column 18 of Kim.

However, this passage cited by the Office Action fails to disclose the "stream identifier"; instead, it relates to what the first bullet on page 3 of the Office Action regards to be the "request message" of claim 1.

The Office Action later acknowledges in the second paragraph on page 4 that "Kim et al. as modified by Zhang et al. still does not teach the control information pair includes a stream identifier."

The Office Action then incorrectly suggests that ITU-T makes up the difference.

First, the Office Action states, (page 4, third paragraph), "ITU-T teaches the control information pair includes a stream identifier (fig. F.7)."

The citation by the Office Action to Figure F.7, however, merely shows a stream ID in a program stream for carrying multimedia.

It is unclear what in ITU-T the Office Action deems to be the "control information pair" of the instant claim 1.

It is accordingly unclear how the statement by the Office Action "ITU-T teaches the control information pair includes a stream identifier (fig. F.7)" could be regarded as correct.

Although data scrambled (Kim, FIG. 21, arrow left to right into the controller 262) may include a program stream that includes a stream ID, the data is not routed to the smart card 261 (see col. 18, lines 46-47: "The signal output to the smart card 261 from recording/digital output controller 262 or IRD 266 is ECM, EMM and CPTC information"; see also acronyms ECM, EMM, CPTC on arrow from controller 262 to smart card 261; see also col. 19, lines 58-65; col. 20, lines 19-21). In particular, the "bit stream output from the IRD" 266 (col. 20, lines 20-21) consists of the control signal "input to smart card 261" (col. 19, line 64). The control signal has "the EMM, ECM and CPTC information" (col. 19, lines 59-60), whereas the "scrambled digital data" (col. 19, line 63) is input "to descrambler 263" (col. 19, line 63) by means of the controller 262 (col. 18, lines 46-47). Since, based on ITU-T, only the Kim scrambled data could fairly be suggested to contain a stream identifier, and since the Kim scrambled data is not sent to the Kim smart card, it is unclear how the Kim smart card can fairly be characterized as sending a reply message containing the stream identifier to the Kim controller 262.

The last paragraph on page 4 of the Office Action appears to suggest that the Kim "ECM contains a content identifier," and cites to lines 61-67 of column 18 in Kim.

Firstly, however, although the passage in Kim the Office Action cites describes alternatives by which the ECM, EMM and CPTC can be combined for transmission, any disclosure or suggestion of a content identifier is absent.

Secondly, it is unclear in what sense a content identifier would be relevant to a stream identifier, the latter expression appearing explicitly in the present claim 1.

The Office Action includes Zhang in the rejection of claim 1, but it is unclear in what manner and by what motivation Zhang could overcome the shortcomings of Kim and ITU-T.

In Zhang, a head-end system 14 sends a stream to a POD module 26. The latter encrypts the stream (col. 10, line 22: "content") using a key and according to a cipher. The POD module 26 then sends the encrypted stream to the host device 24. The host device 24 uses the same key according to the same cipher to decrypt the encrypted stream.

It therefore appears that the Office Action proposes to apply Zhang to modify Kim so that the Kim smart card 261 receives the scrambled data, ECM, EMM, CPTC, i.e., the broadcast stream the Kim now receives (FIG. 21, arrow left to right into controller 262), and so that the Kim smart card forwards the scrambled data to the controller 262 along with the CW and CP.

The present applicants imagine two possibilities for how the Office Action may be combining the references.

According to the first possibility, if the Office Action is suggesting that the broadcast stream in Kim be initially sent to the smart card 261 instead of to the controller 262, it is unclear what in the resulting combination could properly be characterized as the "request message" of the present claim 1.

The second possibility imagined is that the Office Action is implying that Kim be modified, in view of Zhang, so that the broadcast initially arriving at the controller 262 is then sent to the smart card, along with the ECM, EMM, CPTC, and is then sent back to the controller 262, along with the CW and CP. This appears to be an impractical construction.

In particular, with regard to the second possibility, it is at least unclear why it would be obvious to modify Kim to unnecessarily send broadcast content to and back from the smart card 261. To do so, would seem to waste bandwidth and processing resources, without any benefit in return.

In addition, with regard to either possibility, if the fiction of content transmission from the smart cart 261 to the controller 262 could be entertained, it is unclear in what sense any identifier of any stream in the content is paired with either CW or CP to form a "control information pair" which expression appears explicitly in the present claim 1.

For at least the above reasons, it is unclear in what sense, and by what motivation, the combination the Office Action proposes can properly be regarded as featuring all the elements of claim 1. The combination is accordingly deemed not to render obvious the present invention as recited in claim 1.

The Office Action cites, as motivation, providing "authentication of devices as well as keeping data secure."

However, it is unclear to the present applicants how the motivation the Office Action proposes would suggest the combination the Office Action proposes.

The Advisory Action is silent, apparently falling somewhat shy of referring to anything substantive in the Office Action or to any substantive matter in this case whatsoever.

Claim 2 recites, ". . . reply message from the deployment module to the host device, wherein the reply message includes at least one control information pair, each pair having a copy control information and a stream identifier. . . (c) generating a first shared key at the host and a second shared key at the deployment module, respectively, using the at least one control information pair. . ."

Claim 8 recites, ". . . the reply message including at least one control information pair, each pair having copy control information and a stream identifier, generating a first shared key using the at least one control information pair. . ."

Claim 13 recites, ". . . a reply message from the deployment module, wherein the reply message includes at least one control information pair, each pair having copy control information and a stream identifier, generating a second shared key using the at least one control information pair. . ."

Claim 18 recites, ". . . a reply message to the host device, the reply message including at least one control information pair, each pair having copy control information and a stream identifier, generating a first shared key using the at least one control information pair. . ."

Each of claims 2, 8, 13 and 18 is deemed to be patentable over the applied references for at least the reasons set forth above with regard to claim 1.

Rejection of claims 19-21

Claim 19 depends from claim 1, which has been shown to be patentable. . Claim 19 is likewise deemed to be patentable over the applied references for at least this reason.

In addition, claim 19 is separately patentable, at least because it recites, ". . . wherein to use the at least one control information pair in the generating of said second key the set-top box receives a transmission of said at least one control information pair, the respective copy control information of said at least one control information pair not being encrypted for the transmission."

The Office Action applies Zhang to Kim to introduce security concerns for transmission across the POD/host interface, and Zhang encrypts the binding information for transmission from the POD to the host (e.g., col. 8, line 56; col. 12, lines 30-31).

Yet, the Office Action suggests that the combination of references the Office Action cites moves the CP signal across the interface unencrypted.

The applicant does not understand by what reasoning Kim/Zhang can be said to send the binding information across the POD/host interface unencrypted. Motivation cannot be gleaned from the instant patent application, at least because that would amount to impermissible hindsight.

The Office Action cites, as motivation, the idea that foregoing encryption of the binding information results in faster processing.

However, the Office Action applies Zhang to Kim to introduce security concerns for transmission across the POD/host interface. Foregoing encryption, as the Office Action suggests, would degrade security. It is accordingly unclear how Zhang's introduction could fairly be characterized as suggesting that Zhang encryption for transmission across the interface be eliminated. The embodiment the Office Action proposes, which purportedly foregoes encryption for transmission across the interface, would accordingly not have been obvious. Thus, for language particular to claim 19 and, in addition, the reasons set forth above with respect to base claim 1, the combination the Office Action proposes would not have been obvious.

Claim 20 depends from claim 2, which has been shown to be patentable. Claim 20 is likewise deemed to be patentable over the applied references for at least this reason.

In addition, claim 20 is separately patentable, at least because it recites, ". . . wherein step b) is executed without encrypting said copy control information of said at least one control information pair."

Claim 21 depends from claim 8, which has been shown to be patentable. Claim 21 is likewise deemed to be patentable over the applied references for at least this reason.

In addition, claim 21 is separately patentable, at least because it recites, ". . . said copy control information of said at least one control information pair in the reply message is unencrypted upon transmission to the host device."

The remaining rejected claims each depend from one of the base claims and are likewise deemed non-obvious over the cited references for at least the same reason as that asserted for the respective base claim.

In view of the above analysis, it is respectfully submitted that the referenced teachings, whether taken individually or in combination, fail to anticipate or render obvious the subject matter of any of the present claims. Therefore, reversal of all outstanding grounds of rejection is respectfully solicited.

Respectfully submitted,
Dan Piotrowski
Registration No. 42,079

Date: January 17, 2006

By: Steve Cha
Attorney for Applicant
Registration No. 44,069

VIII. CLAIMS APPENDIX

1. (Previously Presented) A system for copy protecting information, the system comprising:

a point of deployment module; and

a set-top box including;

wherein the set-top box transmits a request message for information, the point of deployment module generates a reply message which includes at least one control information pair, relating to the information, each control information pair having copy control information and a stream identifier, respectively generating a first key in the point of deployment module and a second key in the set-top box, using the at least one control information pair, and the point of deployment module encrypting the information with the first shared key and transmitting the encrypted information to the set-top box, and the set-top box decrypting the encrypted information with the second shared key when the first and second shared keys match.

2. (Original) A method of copy protecting information transmitted between a deployment module and a host device, the method comprising the steps of:

(a) transmitting a request message for the information from the host device to the deployment module;

(b) transmitting a reply message from the deployment module to the host device, wherein the reply message includes at least one control information pair, each pair having a copy control information and a stream identifier;

(c) generating a first shared key at the host and a second shared key at the deployment module, respectively, using the at least one control information pair and an encryption means;

(d) encrypting, in the deployment module, the information;

(e) transmitting the encrypted information from the deployment module to the host;

(f) decrypting, at the host, the encrypted information; and

(g) receiving the information at the host when the first and second shared keys match.

3. (Original) The method of claim 2, wherein the deployment module is a point of deployment module.

4. (Original) The method of claim 2, wherein the host is a set-top box.

5. (Original) The method of claim 2, wherein the encryption means includes a hash function.

6. (Original) The method of claim 2, wherein the encrypted information in an elementary stream of information is encrypted with the first shared key.

7. (Original) The method of claim 6, wherein the stream identifier that is transmitted to the host is incorporated with the Packetized Elementary Stream (PES) header of the elementary stream.

8. (Original) A deployment module for use with a host device, the deployment module comprising:

means for communicating with the host device; and

a processor for, in response to a request message for information from the host device, generating a reply message to the host device, the reply message including at least one control information pair, each pair having copy control information and a stream identifier, generating a first shared key using the at least one control information pair, encrypting the information with the first shared key and transmitting the encrypted information to the host device.

9. (Original) The deployment module of claim 8, wherein the deployment module is selected from the group consisting of a point of deployment module, wireless data interface appliance, smartcard, personal computer or internet interface appliance.

10. (Original) The deployment module of claim 9, wherein the host device is a set-top box.

11. (Original) The deployment module of claim 10, wherein the encrypted information is transmitted to the host device using a transport stream, wherein the transport stream includes at least one elementary stream.

12. (Original) The deployment module of claim 11, wherein respective ones of the at least one control information pairs is associated with respective ones of the at least one elementary streams.

13. (Original) A host device for use with a deployment module, the host device comprising:

means for communicating with the deployment module; and

a processor for generating a request message for information to the deployment module, and in response, receiving a reply message from the deployment module, wherein the reply message includes at least one control information pair, each pair having copy control information and a stream identifier, generating a second shared key using the at least one control information pair, and decrypting encrypted information, received from the deployment module, with the second shared key, and receiving the information when the second shared key matches a first shared key generated in the deployment module.

14. (Original) The host device of claim 13, wherein the deployment module is selected from the group consisting of a point of deployment module, wireless data interface appliance, smartcard, personal computer or internet interface appliance.

15. (Original) The host device of claim 14, wherein the host device is a set-top box.

16. (Original) The host device of claim 13, wherein the received encrypted information is included in a transport stream, wherein the transport stream includes at least one elementary stream.

17. (Previously Presented) The host device of claim 16, wherein respective ones of the at least one control information pairs is associated with respective ones of the at least one elementary streams.

18. (Previously Presented) An article of manufacture comprising a computer readable medium in which resides a computer program, said article being part of a deployment module for use with a host device, said program comprising:

instruction means for communicating with the host device; and

instructions for, in response to a request message for information from the host device, generating a reply message to the host device, the reply message including at least one control information pair, each pair having copy control information and a stream identifier, generating a first shared key using the at least one control information pair, encrypting the information with the first shared key and transmitting the encrypted information to the host device.

19. (Previously Presented) The system of claim 1, wherein to use the at least one control information pair in the generating of said second key the set-top box receives a transmission of said at least one control information pair, the respective copy control information of said at least one control information pair not being encrypted for the transmission.

20. (Previously Presented) The method of claim 2, wherein step b) is executed without encrypting said copy control information of said at least one control information pair.

21. (Previously Presented) The deployment module of claim 8, wherein said copy control information of said at least one control information pair in the reply message is unencrypted upon transmission to the host device.

22. (Previously Presented) The deployment module of claim 8, wherein the information to be encrypted comprises content information.

23. (Previously Presented) The deployment module of claim 22, wherein said content information comprises content information of an elementary stream, said stream identifier being an identifier of an elementary stream.

24. (Previously Presented) The system of claim 1, wherein said stream identifier uniquely identifies an elementary stream that is assigned said copy control information.

25. (Previously Presented) The system of claim 24, wherein said stream identifier is within a Packetized Elementary Stream (PES) header of the elementary stream.

26. (Previously Presented) The system of claim 25, wherein the encrypted information to be transmitted to the set-top box includes said header, said set-top box being configured to retrieve said stream identifier from said header.

27. (Previously Presented) The host device of claim 13, wherein said stream identifier uniquely identifies an elementary stream that is assigned said copy control information.

28. (Previously Presented) The host device of claim 27, wherein said stream identifier is within a Packetized Elementary Stream (PES) header of the elementary stream.

29. (Previously Presented) The host device of claim 28, wherein the encrypted information to be received includes said header, said host device being configured to retrieve said stream identifier from said header.

IX. EVIDENCE APPENDIX

The appellants are unaware of any evidence.

X. RELATED PROCEEDING APPENDIX

The appellants are unaware of any related proceedings.